[redacted]

ROUTING AND TRANSMITTAL SLIP Date 16 JULY 1987

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. DIRECTOR OF SECURITY		
2.		
3.		
4.		
5.		

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

#1 - FOR APPROPRIATE HANDLING.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
ADDA	Phone No.

STAT

[redacted]

5041-102 ★U.S.GPO:1985-0-461-274/20011 **OPTIONAL FORM 41 (Rev. 7-76)** Prescribed by GSA FPMR (41 CFR) 101-11.206

Information Security Oversight Office
Washington, DC 20405

CONFIDENTIAL

ISOO-C-87-022

July 6, 1987

ILLEGIB

Dear Mr. Donnelly:

(C) This is an advisory notice regarding security containers. It is intended to advise you of the potential vulnerability of combination lock security containers to new and emerging technological developments; to apprise you of actions being taken to address this issue; and to alert you to consider supplemental precautionary measures that we believe will enhance the protection of national security information.

(U) A number of years ago it was decided among the agencies that are significantly involved in the safeguarding of national security information that combination locks, to be acceptable for this purpose, must protect against surreptitious entry for at least 20 consecutive man-hours. Surreptitious entry refers to the compromise of a security container without leaving physical evidence that the container has been compromised, e.g., manipulating the lock to reveal its combination. Group 1 and Group 1-R combination locks currently used for the protection of national security information were approved on the basis that, among other standards, they would provide the 20 man-hours of protection against surreptitious entry.

(C) Current technologies may have rendered the 20 man-hour standard for Group 1 and Group 1-R locks obsolete. These new technologies are now packaged in devices that are commercially available, relatively inexpensive and easily concealed. While studies of the matter are continuing, some preliminary findings

Classified by: Director, ISOO
Declassify on: OADR

CONFIDENTIAL

indicate that the degree of protection provided by combination locks against surreptitious entry can, through the application of current technology, be diminished to four man-hours or less. Responsible executive branch agencies are currently working to establish conclusively the vulnerability of the current locks, and, as appropriate, develop interim technical countermeasures; to consider anew the appropriate standard for protection against surreptitious entry; and to develop specifications for locks that will meet this and other existing standards. The completion of these tasks may not come quickly.

(C) Following consultation with the member agencies of the Interagency Group/Countermeasures (Policy), the Information Security Oversight Office (ISOO) is now seeking the approval of the National Security Council to enhance the minimum safeguard requirements for Top Secret information stored outside the United States, where the threat from this new vulnerability is believed to be much greater. We enclose a copy of the proposed language. Storage standards published in ISOO Directive No. 1 (32 CFR Part 2001) establish the minimum acceptable levels of protection for classified information. Agencies are always encouraged to establish, by internal regulation, more stringent standards for information under their control.

(C) At present, there are no immediate plans to mandate enhanced minimum storage requirements for national security information within the United States. Until such time as new lock and storage standards are developed and implemented, however, your agency should take those precautionary measures that are feasible without a massive expenditure of additional resources. You should notify appropriate officials within your agency of the increased threat to properly stored classified information; survey your particular threat situations; and, where feasible, protect classified information, especially highly sensitive information, through the application of supplemental countermeasures. For example, in locations where Top Secret information is dispersed, you may wish to consolidate the material in an approved container or vault protected by on-site personnel or an alarm system and response force; or to introduce any other supplemental control that enhances the minimal protection requirements for classified material at that level and below. A classified records clean-out campaign, which disposes of and consolidates classified holdings, is another inexpensive means to reduce the vulnerability. In the course of its program reviews, ISOO will examine those steps that you have taken in response to the increased vulnerability.

(C) The details concerning the vulnerabilities of the Group 1 and Group 1-R locks are classified at the Secret level. This information must be protected accordingly.

(U) If you desire further information, please contact Rudolph Waddy, ISOO Program Analyst, or me at 535-7251 (non-secure). If we do not know the answer to your specific question, we will attempt to put you in touch with someone who does.

Sincerely,

Steven Garfinkel
Director, ISOO

Mr. William F. Donnelly
Deputy Director for Administration
Central Intelligence Agency
Washington, DC 20505

Enclosure

Proposed Change to ISOO Directive No. 1

§ 2001.43 Storage

* * *

(a) Minimum requirements for physical barriers. (1) Top Secret. Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. For Top Secret information stored outside the United States, one or more of the following supplementary controls is required: (i) the area that houses the security container or vault shall be subject to the continuous protection of guard or duty personnel; (ii) guard or duty personnel shall inspect the security container or vault at least once every two hours; or (iii) the security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.